Docket 79744TJS
Customer No. 01333

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of

Kenneth A. Parulski, et al

DIGITAL CAMERA WITH IMAGE AUTHENTICATION

Serial No. 09/473,522

Filed 28 December 1999

Group Art Unit: 2135
Confirmation No. 1080
Examiner: Thomas A. Gyorfi

I hereby certify that this correspondence is being deposited today with the United States Postal Service as first class mail in an envelope addressed to Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Paula West
Paula West

3-29-07
Date

Mail Stop APPEAL BRIEF-PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA. 22313-1450

Sir:

APPEAL BRIEF PURSUANT TO 37 C.F.R. 41.37 and 35 U.S.C. 134

Table of Contents

APPELLANTS' BRIEF ON APPEAL

Appellants hereby appeal to the Board of Patent Appeals and Interferences from the final rejection of claims 1-25 which was contained in the Office Action mailed October 20, 2006.

A timely Notice of Appeal was mailed January 22, 2007, and received in the USPTO on January 25, 2007.

Real Party in Interest

The present application is assigned of record to the Eastman Kodak Company. The Eastman Kodak Company is the real party in interest.

Related Appeals and Interferences

No appeals or interferences are known which will directly affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

Status of the Claims

The present application was filed on December 28, 1999 with claims 1-15. New claims 16-25 were subsequently added by amendment. Claims 1-25 are currently pending, with claims 1, 6-10 and 22 being the independent claims. Claims 1-25 stand rejected under 35 U.S.C. §103(a).

Appendix I provides a clean, double spaced copy of the claims on appeal.

Status of Amendments

There have been no amendments filed subsequent to the appealed final rejection.

Summary of Claimed Subject Matter

Independent claim 1 is directed to an improvement in a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature. The improvement comprises a processor located within the digital camera for generating a random seed entirely from sensor noise within the digital camera and

for using the random seed to generate a private key and a public key, and means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature.

An illustrative embodiment is digital camera 10 shown in FIG. 1. The digital camera 10 includes a processor 18 which creates a public/private key pair, and stores the private key in flash memory 26. See the specification at page 6, lines 12-16, page 8, lines 1-5 and 27-31, page 9, lines 24-25, steps 56 and 58 in FIG. 2, and steps 300 to 340 of FIG. 3. Structure corresponding to the recited means for storing comprises processor 18 operating in conjunction with flash memory 26.

Independent claim 6 is directed to an improvement in a method of producing an image authentication signature in a digital camera employing a private key to encrypt a hash of an image captured by the digital camera. The improvement comprises the steps of generating a random seed entirely from sensor noise in the digital camera and using the random seed to generate a private key in the digital camera, and storing the private key in a memory in the digital camera for subsequent encryption of the hash of the digital image.

An illustrative embodiment of the recited method is shown in steps 56 and 58 of FIG. 2. Steps 300 to 340 of FIG. 3 show a more detailed view of one possible implementation of step 56 of FIG. 2. See the specification at page 6, lines 12-16, page 8, lines 1-5 and 27-31, and page 9, lines 24-25.

Independent claim 7 is directed to a method of authenticating an image captured by a digital camera. The method comprises the steps of generating a random seed entirely from sensor noise in the digital camera and using the random seed to generate a private key and a public key in the digital camera, storing the private key in a memory in the digital camera, communicating the public key to a user, capturing a digital image, hashing the captured digital image in the digital camera to produce an image hash, encrypting the image hash in the digital camera with the private key to produce a digital signature, and authenticating the digital image by hashing the image outside of the digital camera, decrypting the digital signature using the public key to produce a decrypted signature, and comparing

the decrypted signature with the image hash produced outside of the digital camera.

An illustrative embodiment is shown in steps 56 to 78 of FIG. 2. See the specification at page 6, line 5, to page 7, line 9.

Independent claim 8 is directed to a method of manufacturing a digital camera capable of producing a digital signature useful for image authentication, comprising the steps of manufacturing a digital camera with an internal processor for generating a random seed entirely from sensor noise within the digital camera and using the random seed to generate a private key and a public key within the digital camera, storing the public key in a memory in the digital camera and communicating the public key to a camera operator, sending the digital camera to an authentication service, activating the digital camera at the authentication service to produce the private key and public key, registering the public key at the authentication service, and sending the digital camera to a user.

An illustrative embodiment is shown in steps 50 to 58 of FIG. 2. See the specification at page 6, lines 5-8 and 12-16, page 8, lines 1-5, 19-24 and 27-31, and page 9, lines 24-25.

Independent claim 9 is directed to an improvement in a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature and a metadata signature corresponding to one or more metadata values. The improvement comprises a processor located within the digital camera for generating a random seed entirely from sensor noise within the digital camera and for using the random seed to generate a private key and a public key, and means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature and the metadata signature.

An illustrative embodiment is digital camera 10 shown in FIG. 1. The digital camera 10 includes a processor 18 which creates a public/private key pair, and stores the private key in flash memory 26. See the specification at page 6, lines 12-16, page 8, lines 1-5 and 27-31, page 9, lines 24-25, page 10, lines 18-31, steps 56 and 58 in FIG. 2, and steps 300 to 340 of FIG. 3. Structure

corresponding to the recited means for storing comprises processor 18 operating in conjunction with flash memory 26.

Independent claim 10 is directed to a method of producing an image authentication signature in a digital camera, comprising the steps of capturing a digital image, compressing the captured digital image, generating a random seed entirely from sensor noise in the digital camera and using the random seed to generate a private key and a public key in the digital camera, storing the private key in a memory in the digital camera, providing one or more metadata values, hashing the compressed captured digital image and at least one of the metadata values to produce an image hash, and encrypting the image hash to produce the image authentication signature.

An illustrative embodiment is shown in steps 56 to 68 of FIG. 2. See the specification at page 6, lines 5-28.

Independent claim 22 is directed to an improvement in a digital camera of the type employing a private key to encrypt a digital image captured by the digital camera to produce an image authentication signature. The improvement comprises a processor located within the digital camera for generating the private key from a physically random process entirely based on sensor noise within the digital camera, and means for storing the private key in a memory in the digital camera for subsequent use in encryption of the digital image to produce the image authentication signature.

An illustrative embodiment is digital camera 10 shown in FIG. 1. The digital camera 10 includes a processor 18 which creates a public/private key pair, and stores the private key in flash memory 26. See the specification at page 6, lines 12-16, page 8, lines 1-5 and 27-31, page 9, lines 24-25, steps 56 and 58 in FIG. 2, and steps 300 to 340 of FIG. 3. Structure corresponding to the recited means for storing comprises processor 18 operating in conjunction with flash memory 26.

Grounds of Rejection to be Reviewed on Appeal

The following issue is presented for review by the Board of Patent Appeals and Interferences:

Claims 1-25 are rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,167,469 (hereinafter "Safai") in view of U.S. Patent No. 6,788,336 (hereinafter "Silverbrook"), U.S. Patent No. 5,732,138 (hereinafter "Noll"), and RFC1750 by Eastlake et al. entitled "Randomness Recommendations for Security" (hereinafter "Eastlake").

Arguments

Claims 1, 4, 5 and 9-15

Appellants initially note that a proper *prima facie* case of obviousness under §103(a) requires that the cited references must teach or suggest all the claim limitations, and that there be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify or combine the reference teachings. See Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(j).

Appellants submit that the Examiner has failed to establish a proper *prima facie* case of obviousness in the §103(a) rejection of claims 1-25, in that the proposed combination of references fails to teach or suggest all the limitations of the claims, and in that no cogent motivation has been identified for modifying or combining the reference teachings to reach the claimed invention.

As indicated above, independent claim 1 recites a digital camera having a processor that generates a random seed entirely from sensor noise within the digital camera. The processor is further specified as using the random seed to generate a private key and a public key. The private key is stored in a memory in the digital camera for subsequent use in encryption of a hash of a digital image to produce an image authentication signature.

This approach advantageously overcomes a number of problems associated with conventional arrangements. For example, it avoids the serious security concerns that can arise when a manufacturer or user has to generate a private key external to the camera and subsequently load the private key into the

camera. See the specification at page 1, line 20, to page 2, line 16, and page 2, lines 25-30.

With regard to independent claim 1, the Examiner in formulating the §103(a) rejection argues that the combined teachings of Safai, Silverbrook, Noll and Eastlake meet each and every limitation of the claim. The Examiner characterizes Safai as teaching "a processor located within the digital camera for generating [a] private key and a public key," relying on column 4, lines 1-15, column 7, lines 30-40, and claim 29 of Safai. See the final Office Action at page 4, section 4, part (a). Appellants respectfully disagree with this characterization of Safai. There is no teaching or suggestion in Safai to the effect that a private key is generated within a digital camera. At column 16, lines 29-30, Safai indicates that a private key is "stored in the camera," but nowhere does Safai disclose that the private key that is stored in the camera is generated within the camera itself. The portions of the Safai reference relied on by the Examiner in this regard fail to indicate with specificity that the private key is generated within the camera, and to the contrary are entirely consistent with generation of the private key external to the camera as in the conventional arrangements described by Appellants at page 1, line 20, to page 2, line 16, of their specification.

In the final Office Action at page 2, section 2, first paragraph, the Examiner further argues that the teachings in Safai at column 4, lines 9-12, and claim 29, indicate that the generation of the private key in Safai is performed within the digital camera. However, Appellants note that a number of the claims which depend from independent claim 1 in Safai clearly recite operations that do not occur in a digital camera, despite the general recitation in their parent claim. See, for example, claim 23, which states that the transporting step of claim 1 further includes the steps of printing a tangible copy of an image and sending the tangible copy of the image to an addressee. Clearly, these steps do not occur in the digital camera, although the parent claim 1 states that the general method is "in a digital camera." Another example is dependent claim 24, which indicates that the sending step of claim 23, which is part of the transporting step of claim 1, includes sending the tangible copy to the addressee using a common carrier. Again, such a step clearly does not occur in a digital camera. The point of this

argument is that the Examiner cannot reasonably conclude that every step recited in every claim dependent from claim 1 in Safai necessarily occurs in a digital camera. Thus, Appellants submit that there is no teaching in the relied-upon portions of Safai to the effect that the private key disclosed therein is generated in a digital camera.

Furthermore, there is additional evidence in Safai itself that the private key disclosed therein is not generated by a processor of the digital camera 100. For example, Safai at column 16, lines 31-32, indicates that the private key is stored in the digital camera in a manner that prevents recovery. More specifically, the private key is "embedded in firmware within the camera." At column 1, lines 27-31, Safai indicates that such firmware is typically read-only memory (ROM). These teachings would tend to indicate that the private key is generated outside the digital camera and stored in firmware thereof at the time of manufacture. Such an approach is entirely conventional, and particularly problematic, as described by Appellants in the background portion of their specification at page 1, line 20, to page 2, line 4.

Moreover, Appellants note that the recited digital camera processor of claim 1 of the present application uses the random seed to generate both a private key and a public key. As indicated above, the Examiner argues that Safai teaches such a processor located within a digital camera. See the final Office Action at page 4, section 4, part (a), which states that Safai teaches "a processor located within the digital camera for generating [a] private key and a public key." However, the relied-upon portions of Safai do not make any mention whatsoever of generation of a public key using a processor of a digital camera, and to the contrary appear to teach away from such an arrangement. See Safai at, for example, column 16, lines 26-29, which simply indicates that a public key for the digital camera 100 is stored at server 601. There is clearly no processor in the digital camera 100 of Safai that generates both a private key and a public key.

The Examiner in an Advisory Action dated February 9, 2007, argues without any support in the cited references that a public key and a private key must necessarily "be generated simultaneously." Appellants respectfully disagree with this unsupported statement. Although public and private keys are indeed

related, there is no need for such keys to be generated simultaneously with one another, as alleged by the Examiner. Each is generated according to a particular technique, and their generation need not be simultaneous. See, for example, the present specification at page 9, lines 20-23, which indicates that the private key x is generated first, and then the public key y is generated from the private key x using the stated mathematical formula. It is clear that the public key and private key therefore need not be generated simultaneously, as is explicitly alleged by the Examiner. Nor is "the public key . . . implicit in the creation of the private key," which is also alleged by the Examiner in the Advisory Action. There is simply no teaching whatsoever in the cited references to the effect that both a private key and a public key are generated by a processor of a digital camera.

Thus, it appears that the Examiner has mischaracterized the teachings of Safai in formulating the §103(a) rejection, and that Safai would suffer from the very same problems as the conventional arrangements identified by Appellants in their specification.

The Examiner acknowledges certain deficiencies in Safai as applied to claim 1, but argues that these deficiencies are overcome by teachings in Silverbrook, Noll and Eastlake. See the final Office Action at pages 4-6. Appellants respectfully disagree. The collective teachings of Safai, Silverbrook, Noll and Eastlake do not teach or suggest a digital camera having a processor that generates a random seed entirely from sensor noise within the digital camera and then uses the random seed to generate a private key and a public key. Silverbrook at column 204, lines 9-19, references the lava lamp based system of Noll as a potential source of random numbers. Thus, Silverbrook is looking to random sources that are external to the digital camera unit 1 of FIG. 1 in Silverbrook. The lava lamp based system of Noll uses a separate digital camera to photograph lava lamps, and then processes the resulting images to obtain a seed. See Noll at column 4, line 46, to column 5, line 19, and column 6, lines 24-27. It is therefore apparent that Silverbrook is suggesting that a source external to the digital camera unit 1 of FIG. 1 in Silverbrook should be used as a source of random numbers. This is directly contrary to the claimed arrangement in which a digital camera includes a processor that generates a random seed entirely from sensor noise

within the digital camera and then uses the random seed to generate a private key and a public key. Accordingly, it is believed that the relied-upon portions of Silverbrook and Noll actually teach away from the claimed invention.

The Examiner at page 2, last paragraph, to page 3, first paragraph, of the final Office Action further argues that Noll is not limited to lava lamps, but more generally applies to any "chaotic system," citing column 4, lines 43-45, column 6, line 66, to column 7, line 11, and claims 1, 8 and 14 of Noll. However, Appellants are not arguing that Noll is limited to digitized images of lava lamps. What Appellants are arguing is that Silverbrook relies on sources external to a digital camera, and any such source taken from Noll would still be arranged external to the digital camera in Silverbrook. Noll in its general statements and claims teaches that a state of a chaotic system is digitized, but Silverbrook nonetheless teaches to treat any such source from Noll as source of randomness that is external to the digital camera unit 1 of FIG. 1.

The Eastlake reference fails to supplement the above-described deficiencies of Silverbrook, Noll and Safai as applied to claim 1. The relied-upon portion of Eastlake, at section 5.3.1, describes an arrangement in which a computer system uses an external video input supplied from a camera as a source of random bits. Such an arrangement is similar to what is described in Noll, where the output of an image-based system is used as an external source of randomness for another system. See step 600 in the flow diagram in FIG. 6 of Noll, where a seed obtained by processing the images of the lava lamps is used as an external source input to a pseudo-random number generator. See Noll at column 6, lines 21-35. There is no suggestion in Eastlake that the camera use its own sensor noise to generate its own random seed. To the contrary, Eastlake teaches that the camera output is used as an external source input to a separate computer system.

Accordingly, it is believed that the combined teachings of Safai, Silverbrook, Noll and Eastlake fail to meet the limitations of independent claim 1.

Furthermore, it is believed that insufficient objective evidence of motivation to combine Safai, Silverbrook, Noll and Eastlake has been identified by the Examiner.

The Federal Circuit has stated that when patentability turns on the question of obviousness, the obviousness determination "must be based on objective evidence of record" and that "this precedent has been reinforced in myriad decisions, and cannot be dispensed with." In re Sang-Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). Moreover, the Federal Circuit has stated that "conclusory statements" by an examiner fail to adequately address the factual question of motivation, which is material to patentability and cannot be resolved "on subjective belief and unknown authority." Id. at 1343-1344.

The Examiner identifies alleged motivation for the proposed combination of Safai, Silverbrook, Noll and Eastlake at pages 5-6 of the final Office Action. Appellants respectfully submit that the proffered statements of motivation are conclusory in nature or otherwise insufficient. For example, the Examiner at page 5, lines 5-6, indicates that one motivation for the combination would be "to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing." Appellants believe that this alleged motivation goes primarily to the strength of the private and public keys, and not to where they are generated, and therefore fails to address the limitations at issue in the claim. Safai alone, for instance, could increase the strength of its keys against compromise by guessing, by simply using longer key lengths or other similar conventional arrangements. Accordingly, this proffered statement of motivation fails to support the particular combination in question. Points [1] and [2] of page 6, first paragraph, of the final Office Action also appear to relate to strength of the generated keys, and not to where the keys are generated, and thus fail to address the limitations at issue. Furthermore, the Examiner in point [3] on page 6, first paragraph, argues that the proposed combination is motivated because it would "obviate the need . . . to carry additional cumbersome hardware." This is conclusory because it relies on an advantage of the claimed invention as alleged motivation for combination of the references. None of the references themselves provide any objective evidence to support this alleged motivation. As noted above, Silverbrook clearly teaches to use an external random source, such as the lava lamp based system of Noll or some other external source as in Eastlake, which is a direct teaching away from the present invention.

The Examiner further argues in the Advisory Action dated February 9, 2007, that Eastlake motivates the proposed combination because it teaches a "strong portable source of randomness." Appellants respectfully disagree with this characterization of Eastlake. Eastlake at page 10, section 5, mentions that there "might be" some "hope for strong portable randomness in the future." However, at page 14, Eastlake indicates, with emphasis supplied, that even if a separate computer were to receive an input from "a camera with the lens cap on" such data "should not be trusted without some checking in case of hardware failure" and "in any case" will "need to be de-skewed as described elsewhere." This is believed to teach away from the claimed arrangement in which a processor within a digital camera generates a random seed entirely from sensor noise within the digital camera and uses such a random seed to generate a private key and a public key.

Finally, it should be noted that those skilled in the art have had long exposure to the teachings of Eastlake (1994) as well as knowledge of the need for improved cryptographic functionality in digital cameras, and yet none of these skilled artisans have heretofore thought to adapt the Eastlake teachings in the manner that the Examiner alleges would have been obvious. This failure of others to achieve the advantageous arrangements set forth in the present claims constitutes strong evidence of non-obviousness.

It therefore appears that the Examiner in formulating the §103(a) rejection of claim 1 over Safai, Silverbrook, Noll and Eastlake has undertaken a piecemeal reconstruction of the claimed invention based upon impermissible hindsight, given the benefit of the disclosure provided by Appellants.

Independent claims 9 and 10 are believed allowable for reasons similar to those identified above with regard to claim 1.

Dependent claims 4, 5 and 11-15 are believed allowable at least by virtue of their dependence from their respective independent claims.

Claim 2

Dependent claim 2 further recites that the random seed for the private key is produced by processing an image captured from an image sensor of the digital

camera so that the random noise level in the captured image is used in producing the random seed. The Examiner in the final Office Action at page 17, last paragraph, argues that the limitation in question is met by the teachings in Silverbrook at column 173, line 35, to column 175, line 2, column 193, line 25, to column 195, line 25, and column 204, lines 10-20. More specifically, the Examiner characterizes Silverbrook as producing a random seed for a private key by processing an image captured from an image sensor of a digital camera. This is believed to be a mischaracterization of the teachings of Silverbrook. For example, Silverbrook at column 173, lines 46-51, and column 174, lines 60-62, indicates that the seed for the generator of random number R "can be any random number except 0" and "should be gathered from a physically random phenomenon." Contrary to the allegation of the Examiner, Silverbrook does not disclose that random noise level in a captured image is used to produce a random seed. Instead, Silverbrook looks to external sources of randomness, such as the lava lamp based system of Noll, and thus teaches away from the proposed combination of references. Accordingly, it is believed that the limitations of claim 2 are not obvious in view of Safai, Silverbrook, Noll and Eastlake.

Claim 3

Dependent claim 3 recites that the processor causes a variable gain amplifier to be in a high gain condition when an initial test image is captured, where a random noise level in the captured image is used to produce a random seed. The Examiner in the final Office Action at page 18, first paragraph, argues that a processor that causes a variable gain amplifier to be in a high gain condition when an initial test image is captured is shown in column 5, lines 55-60, of Safai. Appellants respectfully disagree. Although the relied-upon portion of Safai refers to a photo processor 208 that receives digital signals from an analog-to-digital converter 206, there is no mention of photo processor 208 causing a variable gain amplifier to be in a high gain condition when an initial test image is captured, as recited in the claim. Accordingly, it is believed that the proposed combination of Safai, Silverbrook, Noll and Eastlake fails to meet the particular limitations of dependent claim 3.

Claim 6

Independent claim 6 calls for generating a random seed entirely from sensor noise in a digital camera and using the random seed to generate a private key in the digital camera. The claim further calls for storing the private key in a memory in the digital camera for subsequent encryption of the hash of the digital image. The Examiner again relies on the combination of Safai, Silverbrook, Noll and Eastlake. However, as outlined above, Safai fails to teach or suggest use of a random seed to generate a private key in a digital camera, but instead suffers from the very problems identified by Appellants in the background portion of their specification at page 1, line 20, to page 2, line 16. The Silverbrook, Noll and Eastlake references fail to supplement this fundamental deficiency of Safai, and teach away from the claimed arrangement by teaching to utilize external sources of randomness as inputs to other systems. Accordingly, it is believed that the collective teachings of Safai, Silverbrook, Noll and Eastlake fail to meet the limitations of claim 6.

Claim 7

Independent claim 7 calls for generating a random seed entirely from sensor noise in a digital camera and using the random seed to generate a private key and a public key in the digital camera. The claim further calls for storing the private key in a memory in the digital camera, and communicating the public key to a user. The Examiner again relies on the combination of Safai, Silverbrook, Noll and Eastlake. However, as outlined above, Safai fails to teach or suggest use of a random seed to generate a private key in a digital camera, but instead suffers from the very problems identified by Appellants in the background portion of their specification at page 1, line 20, to page 2, line 16. The Silverbrook, Noll and Eastlake references fail to supplement this fundamental deficiency of Safai, and teach away from the claimed arrangement by teaching to utilize external sources of randomness.

In addition, as indicated above, independent claim 7 recites generation of both a private key and a public key in a digital camera. In characterizing the Safai

reference in the context of formulating the §103(a) rejection of claim 7, the Examiner argues that Safai teaches the generation of both a private key and a public key within a digital camera. See, for example, page 8, bottom of the page, part (a), of the final Office Action. This is believed to be a clear mischaracterization of Safai. As Appellants described above in the context of claim 1, Safai fails to teach or suggest the generation of a private key within a digital camera, much less the generation of both a private key and a public key within a digital camera. Although Safai makes reference to private and public keys, there is no teaching or suggestion to the effect that both such keys are generated within the digital camera. The Silverbrook, Noll and Eastlake references fail to supplement the fundamental deficiencies of Safai as applied to the independent claims, in that such references at best collectively teach to utilize an external source of randomness as an input to another system.

Moreover, it is noted that claim 7 calls for the communication of a public key, from a digital camera in which it is generated, to a user. The Examiner in the final Office Action at page 8, bottom of the page, part (c), relies on the teachings in column 4, lines 5-15, of Safai. However, this portion of Safai makes no mention whatsoever of communicating a public key generated in a digital camera to a user. Instead, as indicated elsewhere herein, Safai at column 16, lines 26-29, indicates that a public key for the digital camera 100 is stored at server 601.

Accordingly, it is believed that the collective teachings of Safai, Silverbrook, Noll and Eastlake fail to meet the limitations of claim 7.

Claim 8

Independent claim 8 calls for manufacturing a digital camera with an internal processor for generating a random seed entirely from sensor noise within the digital camera and using the random seed to generate a private key and a public key within the digital camera. The claim also calls for storing the public key in a memory in the digital camera and communicating the public key to a camera operator, sending the digital camera to an authentication service, activating the digital camera at the authentication service to produce the private

key and public key, registering the public key at the authentication service, and sending the digital camera to a user.

For the reasons noted above in the context of claim 1, the proposed combination of Safai, Silverbrook, Noll and Eastlake fails to teach or suggest the generation of both a private key and a public key within a digital camera using a random seed generated entirely from sensor noise within the digital camera.

In addition, the Examiner argues that the limitation relating to sending the digital camera to an authentication service is shown in column 15, lines 15-25, of Safai. See the final Office Action at page 11, top of page, part (b). However, this relied-upon portion of Safai makes no mention whatsoever of sending camera 100 anywhere, much less to sending the camera to an authentication service as recited. This portion of Safai relates to sending data or images from the camera to server 601, not to sending the camera itself to an authentication service.

Moreover, the Examiner argues that Safai at column 15, lines 15-25, and column 16, lines 20-40, teaches the recited activation of the digital camera at the authentication service to produce private and public keys. See the final Office Action at page 11, part (c). However, the relied-upon portion makes no mention of activation of a camera at an authentication service such that the camera itself produces private and public keys.

Accordingly, it is believed that the proposed combination of Safai, Silverbrook, Noll and Eastlake fails to meet each and every limitation of claim 8.

Claims 16-21

The Examiner at page 20, last paragraph, of the final Office Action argues with regard to the limitations of claims 16-21 that Safai "discloses firmware memory, wherein the private key is produced using an algorithm stored in the firmware memory," relying on column 7, lines 50-55, of Safai. Appellants respectfully disagree with this characterization of the Safai reference. The portion of Safai relied upon by the Examiner simply indicates that the digital camera 100 comprises firmware memory. There is no teaching or suggestion that such firmware is anything other than conventional firmware, and thus no indication that the firmware stores an algorithm used to produce a private key within the digital

camera. Although the Examiner further relies on additional teachings from Silverbrook with regard to the desirability of keeping secret the manner of generating private keys, such teachings do not overcome the fundamental deficiency of Safai as applied to these claims. That is, Safai and the other art collectively fail to disclose incorporation of a private key generation algorithm in firmware memory of a digital camera, and the limitations at issue are therefore not met.

Claim 22

Independent claim 22 calls for a digital camera comprising a processor located within the digital camera for generating a private key from a physically random process entirely based on sensor noise within the digital camera. The claim further recites means for storing the private key in a memory in the digital camera for subsequent use in encryption of a digital image to produce an image authentication signature. The Examiner again relies on the combination of Safai, Silverbrook, Noll and Eastlake. However, as outlined above, Safai fails to teach or suggest use of a random seed to generate a private key in a digital camera, but instead suffers from the very problems identified by Appellants in the background portion of their specification at page 1, line 20, to page 2, line 16. The Silverbrook, Noll and Eastlake references fail to supplement this fundamental deficiency of Safai, and teach away from the claimed arrangement by teaching to utilize external sources of randomness as inputs to other systems. Accordingly, it is believed that the collective teachings of Safai, Silverbrook, Noll and Eastlake fail to meet the limitations of claim 22.

Claim 23

Dependent claim 23 further recites that the physically random process used to generate the private key is dependent upon a random seed produced from a random noise level in a captured image. The Examiner in the final Office Action at page 21, second paragraph, argues that the limitation in question is met by the teachings in Silverbrook at column 204, lines 10-20. This is believed to be a mischaracterization of the teachings of Silverbrook. For example, Silverbrook at

column 173, lines 46-51, and column 174, lines 60-62, indicates that the seed for the generator of random number R "can be any random number except 0" and "should be gathered from a physically random phenomenon." Contrary to the allegation of the Examiner, Silverbrook does not disclose that random noise level in a captured image is used to produce a random seed. Instead, Silverbrook looks to external sources of randomness, such as the lava lamp based system of Noll, and thus teaches away from the proposed combination of references. Accordingly, it is believed that the limitations of claim 23 are not obvious in view of Safai, Silverbrook, Noll and Eastlake.

Claim 24

Dependent claim 24 recites that the random noise level used to produce the random seed is produced by random dark field image data taken from the image sensor. The Examiner in the final Office Action at page 21, last paragraph, to page 22, first paragraph, argues that the limitation is met by admitted prior art or Eastlake. Appellants respectfully disagree. First, Appellants have not admitted that a random noise level used to produce a random seed in a digital camera is produced by random dark field image data taken from an image sensor of that camera. Second, with regard to Eastlake, the relied-upon portion of that reference teaches that input from a "camera with the lens cap on" is supplied to an external computer for "checking" and "to be de-skewed," and that without such additional external operations the random noise from the camera "should not be trusted." This is a direct teaching away from the limitations in question. Accordingly, it is believed that the limitations of claim 24 are not obvious in view of Safai, Silverbrook, Noll and Eastlake.

Claim 25

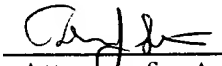
Dependent claim 25 recites that the processor causes a variable gain amplifier to be in a high gain condition when random dark field image data is captured, where the random dark field image data is used to generate a private key in a digital camera. The Examiner in the final Office Action at page 18, first paragraph, argues that a processor that causes a variable gain amplifier to be in a

high gain condition when random dark field image data is captured is shown in column 5, lines 55-60, of Safai. Appellants respectfully disagree. Although the relied-upon portion of Safai refers to a photo processor 208 that receives digital signals from an analog-to-digital converter 206, there is no mention of photo processor 208 causing a variable gain amplifier to be in a high gain condition when random dark field image data is captured, as recited in the claim. Accordingly, it is believed that the proposed combination of Safai, Silverbrook, Noll and Eastlake fails to meet the particular limitations of dependent claim 25.

Conclusion

For the above reasons, Appellants respectfully request that the Board of Patent Appeals and Interferences reverse the rejection by the Examiner and mandate the allowance of claims 1-25.

Respectfully submitted,



Thomas J. Strouse/phw
Telephone: 585-588-2728
Facsimile: 585-477-4646
Attorney for Appellants
Registration No. 53,950
Enclosures
If the Examiner is unable to reach the Appellants' Attorney at the telephone number provided, the Examiner is requested to communicate with Eastman Kodak Company Patent Operations at (585) 477-4656.

Appendix I - Claims on Appeal

1. In a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature, the improvement comprising:

(a) a processor located within the digital camera for generating a random seed entirely from sensor noise within the digital camera and for using the random seed to generate a private key and a public key; and

(b) means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature.

2. The digital camera claimed in claim 1, further including an image sensor for capturing images, and wherein the processor includes means for producing a random seed for the private key by processing an image captured from the image sensor so that the random noise level in the captured image is used in producing the random seed.

3. The digital camera according to claim 2, further including:

(i) a variable gain amplifier coupled to the image sensor;

(ii) an analog-to-digital converter coupled to the variable gain amplifier and the processor for producing digital signals corresponding to the captured images; and

(iii) the processor causing the variable gain amplifier to be in a high gain condition when the initial test image is captured.

4. The digital camera claimed in claim 1, wherein the processor includes one or more algorithms for producing the random seed, wherein the random seed is used to produce a random number k, and for using the random number k to create the image authentication signature by hashing the raw image data prior to image processing.

5. The digital camera claimed in claim 4, wherein the processor includes an image processing algorithm which uses JPEG compression.

6. In a method of producing an image authentication signature in a digital camera employing a private key to encrypt a hash of an image captured by the digital camera, the improvement comprising the steps of:

(a) generating a random seed entirely from sensor noise in the digital camera and using the random seed to generate a private key in the digital camera; and

(b) storing the private key in a memory in the digital camera for subsequent encryption of the hash of the digital image.

7. A method of authenticating an image captured by a digital camera, comprising the steps of:

(a) generating a random seed entirely from sensor noise in the digital camera and using the random seed to generate a private key and a public key in the digital camera;

(b) storing the private key in a memory in the digital camera;

(c) communicating the public key to a user;

(d) capturing a digital image;

(e) hashing the captured digital image in the digital camera to produce an image hash;

(f) encrypting the image hash in the digital camera with the private key to produce a digital signature; and

(g) authenticating the digital image by hashing the image outside of the digital camera, decrypting the digital signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera.

8. A method of manufacturing a digital camera capable of producing a digital signature useful for image authentication, comprising the steps of:

(a) manufacturing a digital camera with an internal processor for generating a random seed entirely from sensor noise within the digital camera and using the random seed to generate a private key and a public key within the digital camera, storing the public key in a memory in the digital camera and communicating the public key to a camera operator;

(b) sending the digital camera to an authentication service;

(c) activating the digital camera at the authentication service to produce the private key and public key, and registering the public key at the authentication service; and

(d) sending the digital camera to a user.

9. In a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature and a metadata signature corresponding to one or more metadata values, the improvement comprising:

(a) a processor located within the digital camera for generating a random seed entirely from sensor noise within the digital camera and for using the random seed to generate a private key and a public key; and

(b) means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature and the metadata signature.

10. A method of producing an image authentication signature in a digital camera, comprising the steps of:

(a) capturing a digital image;

(b) compressing the captured digital image;

(c) generating a random seed entirely from sensor noise in the digital camera and using the random seed to generate a private key and a public key in the digital camera;

(d) storing the private key in a memory in the digital camera;

(e) providing one or more metadata values;

(f) hashing the compressed captured digital image and at least one of the metadata values to produce an image hash; and

(g) encrypting the image hash to produce the image authentication signature.

11. The method according to claim 10 further including the step of storing in an image file in the digital camera, the image authentication signature, the compressed digital image data, and the one or more metadata values.

12. The method according to claim 10 wherein the encrypting step includes encrypting the image hash with a private key produced in the digital camera to produce the image authentication signature.

13. The method according to claim 10 wherein the encrypting step includes encrypting the image hash with the private key to produce the image authentication signature; and further including the step of:

authenticating the captured digital image by hashing the compressed digital image outside of the digital camera, decrypting the image authentication signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera.

14. The method according to claim 10 further including the steps of: hashing the uncompressed captured digital image to produce a random number *k*; and wherein the encrypting step includes using the random number *k* to produce the image authentication signature.

15. The method according to claim 10 wherein the encrypting step further produces a metadata signature corresponding to the one or more metadata values.

16. The digital camera according to claim 1, further including firmware memory, wherein the private key is produced using an algorithm stored in the firmware memory and wherein the algorithm is deleted from the firmware memory after the private key is generated.

17. The method according to claim 6, wherein the private key is produced using an algorithm stored in firmware memory in the digital camera, and wherein the algorithm is deleted from the firmware memory after the private key is generated.

18. The method according to claim 7, wherein the private key is produced using an algorithm stored in firmware memory in the digital camera, and wherein the algorithm is deleted from the firmware memory after the private key is generated.

19. The method according to claim 8, wherein the private key is produced using an algorithm stored in firmware memory in the digital camera, and wherein the algorithm is deleted from the firmware memory after the private key is generated.

20. The digital camera according to claim 9, further including firmware memory, wherein the private key is produced using an algorithm stored in the firmware memory and wherein the algorithm is deleted from the firmware memory after the private key is generated.

21. The method according to claim 10, wherein the private key is produced using an algorithm stored in firmware memory in the digital camera, and wherein the algorithm is deleted from the firmware memory after the private key is generated.

22. In a digital camera of the type employing a private key to encrypt a digital image captured by the digital camera to produce an image authentication signature, the improvement comprising:

(a) a processor located within the digital camera for generating the private key from a physically random process entirely based on sensor noise within the digital camera; and

(b) means for storing the private key in a memory in the digital camera for subsequent use in encryption of the digital image to produce the image authentication signature.

23. The digital camera claimed in claim 22, further including an image sensor for capturing images, and wherein the physically random process is dependent upon a random seed produced from a random noise level in a captured image.

24. The digital camera claimed in claim 23 wherein the random noise level is produced by random dark field image data taken from the sensor.

25. The digital camera according to claim 24, further including:

(i) a variable gain amplifier coupled to the image sensor;

(ii) an analog-to-digital converter coupled to the variable gain amplifier and the processor for producing digital signals corresponding to the captured images; and

(iii) the processor causing the variable gain amplifier to be in a high gain condition when the random dark field image data is captured.

Appendix II - Evidence

None

Appendix III – Related Proceedings

None